The official voice of the Air Force Research Laboratory
news@afrl
Features
February 2004

Rome lab documents threats to infrastructure

by Francis L. Crumb, Information Directorate

ROME, N.Y. — The analyses of threats to the North American electrical power grid, financial sector and rail system is included in a report on current cyber threats to critical infrastructure recently delivered to the Air Force Research Laboratory's Information Directorate.

The National Institute of Justice's CyberScience Laboratory at the Rome Research Site prepared the comprehensive study of selected critical infrastructures to provide an operational context to current and emerging cyberthreats. The research was performed by Dolphin Technology Inc. at Griffiss Business & Technology Park, and subcontractor WetStone Technologies Inc. of Cortland.

"Critical infrastructure within the U.S. is vulnerable to cybersecurity threats," said Glen E. Bahr, program manager in the directorate's Defensive Information Warfare Branch. "The rapid advances in technology available to the general public off-the-shelf and at affordable cost, plus worldwide improvements in communications technology that convey cyberthreats internet-wide, demand that both military and law enforcement professionals be apprised of current threats and risks, and be up to date on information assurance security requirements."

Dolphin Technology and WetStone provided directorate engineers with an assessment of current state-of-the-art information assurance tools, technology and techniques to include vulnerability, response and recovery capabilities.

"This is a study in progress, but we have received some significant early reports," Mr. Bahr said. "Those reports will be shared with authorities that need them through NIJ's National Law Enforcement and Corrections Technology Center Northeast Region here at Rome." The report is part of an ongoing study that has relevance to the Departments of Defense. The next step in the program will be for Dolphin Technology to address potential gaps in cybersecurity and related infrastructure protection.

The NIJ's Office of Science and Technology established the CyberScience Laboratory (CSL) in March of 2000, as part of its National Law Enforcement and Corrections Technology Center (NLECTC) Northeast Region, which is co-located with the AFRL Information Directorate. Since that time, the CSL has been on the forefront in the battle against cybercrime.

The mission of the CyberScience Laboratory is to develop a national government, industry, and academic collaboration to address cybercrime technical issues and to share a forensic tool knowledge base with the NLECTC system, state crime laboratories and state and local law enforcement agencies across the country. It also seeks to heighten national awareness of cybercrime, as well as provide technology assistance and facilitate cybercrime training for local law enforcement agencies. @